## REMARKS

Claims 1 – 15 are presently pending in the application. Claims 1 and 11 have been amended to clarify the invention. No new matter has been added and support for the amendments to the claims can be found in the specification and drawings. Applicants are submitting formal drawings herewith which correct the deficiencies noted by the Examiner in the Office Action. In view of the above claim amendments and arguments for patentability presented hereinbelow, Applicants respectfully submit that the application is now in condition for allowance.

### Claim Rejections – 35 U.S.C. § 102(e)

Claims 1 and 4-15 stand rejected under section 102(e) as being anticipated by Garrison U.S. Patent No. 6,275,939 ("Garrison"). Applicants respectfully traverse this rejection and submit that Garrison fails to disclose or suggest the claimed invention.

In accordance with an aspect of the invention, there is provided a system and method of using a Virtual Single Account (VSA) that can significantly improve the convenience and security performance for mobile users who remotely access office networks via various local access networks. A mobile computing device is provided with client software/and or hardware that manages local and remote network information, provides automatic local and remote access services for the mobile host, and communicates with external VSA servers to obtain local and remote access information updates. The invention improves security for mobile users as well as local access networks and office networks, by using encrypted authentication credentials, such that the mobile user doesn't have knowledge of the authentication credentials. The invention does not require any changes to existing local access networks, thereby facilitating maximum interoperability between office networks that support remote access and local access networks that provide IP connectivity. The only requirement regarding local access networks is that VSA system administrators be able to open, modify, and close accounts as ordinary users. Such basic functions are invariably supported by local access networks. The VSA system and method gives system administrators the flexibility to selectively configure a mobile user's VSA client,

such that the user can only connect to an office network via a specific subset of existing local access networks.

In accordance with an aspect of the invention, a mobile user only needs to remember a single authentication credential (hereafter it is assumed to be a username/password pair for simplicity) for one account (i.e., a VSA), managed by an administrator in the user's office network. The user's mobile computing device (hereinafter, a "mobile host") is provided with client software/and or hardware (hereinafter, "a VSA client") that manages local and remote network information, provides automatic local and remote access services for the mobile host, and communicates with external VSA servers to obtain local and remote access information updates. After the user supplies the correct username and single password to the VSA client, the VSA client operates to automatically authenticate the user and connect the user's mobile device to a current local access network, and then automatically authenticates the user and connects the mobile device to the user's office network. In this regard, the mobile host's connection to the office network can be maintained as the user "roams" and thus all networking application programs can continue running when the user moves from the coverage of one access network to another access network. All authentication credentials are encrypted using a key generated from the user's VSA password. The user supplies a single password to initiate the connection procedure, and the VSA client derives the key from the submitted VSA password and decrypts all authentication credentials that are needed in order to connect the mobile device to current local access network and then to the office network. Accordingly, even if someone steals the user's VSA username and password, local and remote network access cannot be obtained without possessing the user's mobile host (specifically, the encrypted authentication credentials managed by the VSA client).

Representative claim 1, as amended, calls for:

> A client for connecting a mobile host to a remote network through an access network with a single user password, where the access network may be independent of the remote network in terms of no protocol conversation between authentication servers in the access network and the remote network, respectively, and a virtual single account (VSA) has been set up for a user to connect to the

access network and then to the remote network, the client comprising machine readable instructions stored in a memory medium, which when executed by a processor:

generate a VSA password and decryption key from the single password received from the user;

decrypt at least one of a local access network authentication credential and a remote access authentication credential *stored in encrypted form in the memory medium*;

initiate a local access network connection; and

initiate a remote network access connection.

Emphasis added.

Turning now to Garrison, that reference discloses a system and method for securely *accessing a database* from a remote location. As described in Garrison:

> The present invention utilizes a client computer (client), a server computer (server), and a database system. The client establishes communication with the server from a remote location and submits a request for data to the server. *The server translates the request for data into a query for the database system.* The server queries the database system with the translated query, and in response, the database system retrieves the requested data and transmits the requested data to the server. *The server encrypts the requested data and transmits the encrypted data to the client.*
>
> If part of the data requested by the client is not stored in the database system associated with the server, the server creates a request for data and sends the request for data to a remote server. The remote server translates the request for data into another query and queries a database system associated with the remote server. The remote server then transmits the data retrieved from the database system associated with the remote server to the server. The server then assimilates all of the retrieved data and transmits the retrieved data in encrypted form to the client. The server may query a plurality of remote servers in order to retrieve all of the information requested by the client.
>
> *In accordance with another feature of the present invention, the client initially transmits a password to the server in order to identify the user of the client as an authorized user. The server translates the password into a different password (an "alias" password) and utilizes the alias password to gain access to the database system.*

> In accordance with another feature of the present invention, the server transmits a new encryption key to the client each time the client establishes a data session with the server. Thereafter, the client and server encrypt all information communicated therebetween in the data session with the new encryption key. Col. 2, line 42 – Col. 3, line 2 (emphasis added).

It is axiomatic that in order to support a proper Section 102 rejection, every element in the claim must be found in the cited reference. Applicants submit Garrison fails to support a proper section 102 rejection as several elements found in claim 1 are not disclosed in the cited reference, and further that Garrison fails to suggest the claimed invention.

In Applicants' system, authentication credentials for access to a *local access network* and a *remote network* are *stored on a user's mobile device in encrypted form* and are *decrypted on that device* using a key generated from the user's VSA password. The user supplies a single password to initiate the connection procedure, and the VSA client derives the key from the submitted VSA password and decrypts all authentication credentials that are needed in order to connect the mobile device to current local access network and then to the remote (e.g., office) network. Accordingly, even if someone steals the user's VSA username and password, local and remote network access cannot be obtained without possessing the user's mobile host (specifically, the encrypted authentication credentials managed by the VSA client). Garrison fails to disclose or suggest such an arrangement.

Garrison is directed to a system that provides secure access to a database from a remote location. In this regard, a client initially transmits a password to a server in order to authenticate the client to that server. The server then translates the password into an "alias password" that is utilized to obtain access to the target database. See Col. 2, line 64 – Col. 3, line 2. Encryption is utilized to protect communications between the server and the client. As stated in Garrison "[t]he server translates the request for data into a query for the database system. The server queries the database system with the translated query, and in response, the database system retrieves the requested data and transmits the requested data to the server. *The server encrypts the requested data and transmits the requested*

*data to the client.*" Col. 2, lines 45 – 51 (emphasis added). Garrison's disclosure of encrypted communications is inapposite to the present invention.

There is nothing in Garrison that is teaches or suggests obtaining access to a local access network and a remote access network in the manner claimed by Applicants. Garrison merely provides access to a database via a server from a remote location. Furthermore, Garrison fails to disclose or suggest storing authentication credentials for local and remote access networks on a mobile host in an encrypted form, where such credentials are decrypted by the mobile host with a decryption key that is generated from a single user password. Garrison only stands for the proposition that communications between the server and client may be encrypted. See Col. 2, lines 51- 52 and Col. 3, lines 3 – 8 (every time a data session is established between the client and server a new encryption key is sent to the client to protect the information). Garrison does not store any encrypted authentication credentials on a mobile host that are decrypted upon receipt of a user password that is used to generate a decryption key. By way of contrast, Garrison merely transmits a password to the server to provide initial authentication, and the server then generates another password from the first password to obtain access to the database. This has nothing to do with what is being claimed here.

In view of the above, it is respectfully submitted that independent claim 1 is patentable over Garrison, and that those claims that ultimately dependent on claim 1 are also patentable for at least the same reasons.

With respect to independent claim 11, Applicants respectfully disagree with the Examiner's position. For example, the Examiner contends that the step of "send a VSA information update response message to the mobile host in response to receiving a VSA information update request message from the mobile host" is met at Col. 2, lines 52-59. Applicants have amended claim 11 to clarify the invention in that the VSA update response message includes *current remote access parameters for the remote network.* Garrison is devoid of any teaching or suggestion of this feature. Garrison also fails to meet the step of "verify[ing] an authentication credential for the remote network received from the mobile host." The citation to Col. 2, line 64 – Col. 3, line 2 describes access to a database, not a

remote network within the context of the present invention. Similarly, the last step -- "authorize a remote gateway in the remote network to connect the mobile host to the remote network," is not taught or suggested in Garrison. Accordingly, it is submitted that independent claim 11 is patentable over Garrison, and that those claims that ultimately depend from claim 11 are patentable over Garrison for at least the same reasons.

**Claim Rejections – 35 U.S.C. § 103(a)**

Claims 2 and 3 stand rejected under Section 103(a) as being unpatentable over Garrison in view of Cohen et al. U.S. Patent No. 6,178,511 ("Cohen"). Applicants hereby reiterate the above argument distinguishing Garrison from the claimed invention and submit that the addition of Cohen fails to remedy the deficiencies in the disclosure of Garrison.

As disclosed in Cohen:

> The present invention implements a single sign-on (SSO) mechanism that coordinates logois [sic] to local and remote resources in a computer enterprise with preferably one ID and password.
>
> More specifically, this invention provides a single sign-on (SSO) framework that allow users to sign on to a client system one time entering ones password. The SSO framework then signs on to other applications on the user's behalf.
>
> The SSO framework supports storage of all passwords and keys belonging to a user in secure storage (e.g., either in local storage, a centralized password service, a smartcard, or the like), so that the user needs to remember only one ID and password. Upon authentication, the SSO mechanism securely retrieves all the passwords for a user from the secure storage and automatically (i.e. without additional user intervention) issues sign-ons to each system/application the user is authorized to access. Col. 2, lines 24 – 41.

Cohen fails to disclose or suggest any of the following steps: "decrypt at least one of a local access network authentication credential and a remote access authentication credential *stored in encrypted form in the memory medium* [on the mobile host]; initiate a local access network connection; and initiate a remote network access connection." In Cohen, passwords for logging onto a plurality of

different computer systems are stored in a personal key manager 24 (see Col. 4, line 61 – col. 5, line 6. There is absolutely no mention of decrypting authentication credentials on a mobile host and using those credentials to authenticate to a local access network and a remote network. Furthermore, the fact that Cohen teaches updating the "configuration information manager (CIM)" 22 is irrelevant to the claimed invention (see the Examiner's citation to a "configuration update process" at Col. 4, lines 48-60). Accordingly, it is respectfully submitted that even if, assuming *arguendo*, Garrison and Cohen are properly combinable, such combination would still fail to reach the claimed invention.

In view of the foregoing, Applicants respectfully submit that claims 1 – 15 are patentable over the cited art and allowance of these claims at an early date is solicited.

The Office is hereby authorized to charge any additional fees or credit any overpayments under 37 C.F.R. 1.16 or 1.17 to AT&T Corp. Account No. 01-2745. The Examiner is invited to contact the undersigned at (908) 707-1573 to discuss any matter concerning this application.

Respectfully submitted,
Paul Shala Henry, et al.
By:

Date: 6/17/05

Gary H. Monka
Registration No. 35,290
Attorney for Applicant

Canavan & Monka, LLC.
250 State Route 28, Suite 207
Bridgewater, New Jersey 08807
(908) 707-1573